REMARKS

Claims 1, 3-7, 9, 10, 17, and 21-31 are pending in the present application. By this Response, claims 1, 17 and 28 are amended. Reconsideration of the claims is respectfully requested in view of the following remarks.

I. Telephone Interview

Applicant's representative contacted the Examiner to conduct a telephone interview prior to the response due date of the Office Action. However, a telephone interview was not able to be scheduled prior to the response due date. Therefore, Applicant respectfully requests that the Examiner contact Applicant's representative to discuss this application prior to taking any further action on this case.

II. Rejection under 35 U.S.C. § 103(a) Based on Li and Deo

The Office Action rejects claims 1, 3-7, 9, 10, 21-23, and 25-31 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Li et al. (Patent WO 98/26540) in view of Deo et al. (U.S. Patent No. 5,721,781). This rejection is respectfully traversed.

Claim 1, which is representative of the other rejected independent claims with regard to similarly recited subject matter, reads as follows:

> 1. A method, in a data processing system, for providing a system administrator with a view of a plurality of applications accessible by a user, comprising:
>
> receiving, in the data processing system, ***in response to a coupling of a separate hardware security device to the data processing system, credential information comprising user names and associated passwords for each application of the plurality of applications that the user uses, from the separate hardware security device into an authentication credential container associated with the user;***
>
> ***identifying, by the data processing system, the plurality of applications accessible by the user by examining the authentication credential container associated with the user;***

generating, by the data processing system, a view of the plurality of applications accessible by the user, wherein the view is a consolidated user directory that contains user authentication information across the plurality of applications; and

displaying, by the data processing system, the view to the administrator.

(emphasis added)

Applicant respectfully submits that neither the Li nor the Deo references, either alone or in combination, teach or render obvious at least the features of claim 1 emphasized above, or the similar features found in the other independent claims 17 and 28.

Li is directed to a centralized database system for automatically generating a new user form for setting up services by copying default settings from a template into the new user form for the services. With the mechanism of Li, an agent registry in a central database is queried to determine available services and then those available services (represented as agents) copy default settings into a new user form. In addition, default settings from a selected user template may be copied into the new user form and may override any conflicting default settings from the available services (represented as agents). As a result, a central, integrated database holds all the settings for a particular user for all services available within a computer system (see page 3, lines 13-21; page 13, lines 23-34; page 14, lines 5-10).

Thus, Li is directed to generating, in a centralized database, a new user form based on default values for services obtained from agents and selected user templates. The new user form may then be used for setting the values for the various services when a user logs onto the computer system.

Nowhere in Li is there any teaching or technical rationale provided to implement the feature of receiving, ***in response to a coupling of a separate hardware security device to the data processing system***, credential information comprising user names and associated passwords for each application of the plurality of applications that the user uses, ***from the separate hardware security device into an authentication credential container associated with the user***. As recognized by the Office Action, Li does not even mention a separate hardware security device, let alone coupling a separate hardware security device to a data processing system and, in response to such coupling, receiving

in the data processing system credential information for each application of a plurality of applications that a user uses. To the contrary, Li is only concerned with using established templates in a centralized database to generate a new user form in the centralized database based on the default values specified in the established templates. Thus, everything in Li happens at a centralized database, not between a separate security device and a data processing system. That is, Li does not receive credential information from a separate security device upon coupling of the separate security device with a data processing system. Moreover, Li does not receive credential information for a plurality of applications that a user uses.

Furthermore, Li does not teach or provide any technical rationale to identify a plurality of applications accessible by the user ***by examining the authentication credential container associated with the user***. Li teaches a user form that stores the setting values for the services for a user, but this user form is not an authentication credential container as recited in the present claim because the user form in Li does not receive credential information for each of a plurality of applications from a separate hardware security device in response to the separate hardware security device being coupled to a data processing system. Thus, even though Li teaches a user form that stores setting data for services for a particular user, this user form is not the same as the credential container recited in claim 1.

With regard to identifying the plurality of applications by examining the authentication credential container, the Office Action alleges that this feature is taught by Li at page 8, lines 22-30. In actuality, this section of Li only teaches that an account database provides a central location for all the parameters and settings for particular services within a computer system for each user of that system and that this is preferred because of the reduction in duplication, more efficient administration, and more efficient addition, modification, and deletion of user accounts. There is nothing in the cited section of Li, or any other section of Li, that teaches or renders obvious the specific features of identifying a plurality of applications accessible by the user by examining the authentication credential container associated with the user, the authentication credential container being populated with authentication information from a separate hardware device as recited in claim 1.

Moreover, Deo does not teach or provide any technical rationale to implement these features either. Deo is directed to a system for authenticating a smart card and its stored applications. With the mechanism of Deo, a smart card is assigned its own digital certificate and each of the applications stored on the smart card are assigned their own digital certificate. During a transaction with a terminal, which also has its own certificate and whose application also has its own certificate, the smart card and the terminal exchange their certificates to authenticate one another. A smart card application is then selected and its related certificate and the certificate of a terminal application are exchanged in order to authenticate the applications. A PIN is entered by a user to authenticate the user. Thus, Deo is directed to a mechanism for authenticating the smart card and applications as being authentic, as well as authenticating a user via a PIN as being an authentic user for using the smart card.

Deo does not teach, or provide any technical rationale to implement, the features of receiving, in the data processing system, in response to a coupling of a separate hardware security device to the data processing system, credential information comprising user names and associated passwords for each application of the plurality of applications that the user uses, from the separate hardware security device into an authentication credential container associated with the user. To the contrary, in Deo, the authentication simply authenticates the smart card, a selected application on the smart card, the terminal, the terminal application, and the user. The smart card in Deo does not transfer from the smart card to the terminal, user names and passwords for each of a plurality of applications that a user uses, which are then stored in an authentication credential container associated with the user. All Deo teaches is authenticating the smart card based on a certificate associated with the smart card, authenticating a selected smart card application on the smart card using a certificate associated with the smart card application, authenticating the terminal and terminal application based on certificates associated with the terminal and terminal application, and authenticating the user based on a PIN.

Moreover, there is no ability in Deo to identify a plurality of applications accessible by a user by examining an authentication credential container associated with the user. Deo does not even teach such an authentication credential container since it is

only concerned with the immediate authentication of the smart card, smart card application, terminal, terminal application, and user based on certificates and a PIN. Deo is not concerned with transferring authentication information, comprising user names and passwords, for a plurality of applications used by a user, from a separate security device to a data processing system for storage in an authentication credential container associated with a user, let alone examining such an authentication credential container to identify what applications are accessible by a user.

Since neither reference alone teaches or renders obvious these features of claim 1, any alleged combination of the references also would not result in these features being taught or rendered obvious. Moreover, one of ordinary skill in the art would not have been motivated to combine the references as alleged by the Office Action because the references are directed to completely different and incompatible mechanisms for solving completely different and unrelated problems.

Li is concerned with making the setup of users in a computer system more automated by providing a mechanism for creating a new user form from templates of default values and then using the user form to register the user with services. The problem addressed is the fact that user registration was a manual process in the past and the Li mechanism provides a more automated user registration mechanism.

Deo is concerned with making smart card transactions more secure by providing a three-tier authentication system. The problem addressed by Deo is increasing security of smart card transactions by not only authenticating the smart card and user, but also the smart card application, the terminal, and the terminal application.

Increasing security of smart card transactions has nothing to do with automating a process for registering users with services. These are two separate and distinct problems with two separate and distinct solutions provided by the two references. There is no reason why one of ordinary skill in the art would look at either of these references as a solution for a problem associated with the other reference and thus, there would be no reason to even attempt to combine the teachings of these references. Moreover, even if one were somehow motivated to combine these references for some reason, *arguendo*, the result would not be the invention as recited in claim 1. To the contrary, the result of the combination would be some centralized database system in which user forms are

generated using templates and default values in the templates as a way of registering a user with services (Li), and in which a three tier smart card authentication mechanism is used to authenticate a transaction between a user using a smart card and a terminal (Deo). The result would not be a mechanism such as recited in claim 1 or the other rejected independent claims.

In view of the above, Applicant respectfully submits that the alleged combination of Li and Deo does not teach or render obvious the invention as recited in independent claims 1, 17, and 28. At least by virtue of their dependency on claims 1, 17, and 28, the alleged combination of references fails to teach or render obvious the features of dependent claims 3-7, 9, 10, 21-23, and 25-27, and 29-31. Accordingly, Applicant respectfully requests withdrawal of the rejection of claims 1, 3-7, 9, 10, 17, 21-23, and 25-31 under 35 U.S.C. § 103(a).

In addition to their dependency, the alleged combination of references fails to teach or render obvious the specific features of the dependent claims. For example, with regard to claim 3, the alleged combination of references fails to teach or render obvious the features of removing access to an application from the plurality of the applications by ***utilizing the view of the plurality of the applications accessible by the user***. The Office Action alleges that this feature is taught by Li at page 8, lines 4-11, page 10, lines 29-33, and page 13, lines 15-20. Page 8, lines 4-11 of Li teaches that a system administrator module provides a GUI for accessing an Internet access device in order to manage e-mail and web pages, perform system administration, allow access by individual users, and monitor and support the functioning of the Internet device. Page 10, lines 29-33 of Li merely teaches a user interface for adding, editing, and deleting users from a system. Page 13, lines 15-20 teaches a user interface for deleting a user including a message window, confirmation window, and command buttons.

While Li may teach a GUI for deleting a user from a system, the GUI used in Li is not a view of a plurality of applications as generated in the way recited in the presently claimed invention. Moreover, the GUI in Li is for deleting the user from the system, not removing access by a user to an application from a plurality of applications. In other words, with Li, the user is completely removed from the system and thus, all of the user's access to all applications is removed. There is no teaching in Li of a GUI that allows one

to remove a user's access to a particular application in a plurality of applications. Thus, Li does not in fact teach or render obvious the features of claim 3, contrary to the allegations raised in the Office Action.

With regard to claim 4, the alleged combination of references fails to teach or render obvious the features of creating a user account for a new application to be accessible by the user ***utilizing the generated view***; and injecting authentication information of the user account ***into the authentication credential container*** of the user. Again, as discussed above, neither reference teaches or renders obvious the authentication credential container as it is recited in the present claims. The user form in Li is not the same as an authentication credential container for the reasons previously mentioned above. Thus, Li cannot be found to teach injecting authentication information into such an authentication credential container. Moreover, the Office Action agrees that Li does not teach injecting authentication information (see Office Action, page 6) but alleges that Deo teaches this feature at column 2, lines 60-65, column 3, lines 10-15 and 18-23.

Column 2, lines 60-65 of Deo teaches that the smart card has its own certificate and each of the smart card applications have their own certificate. Column 3, lines 10-15 teaches that the smart card and the terminal each process the other's certificate to verify authenticity of the other and a security communication path is established. Column 3, lines 18-23 teaches that an application is selected and application-related certificates of the smart card application and terminal application are exchanged and authenticated. There is nothing in these portions of Deo that says anything regarding injecting authentication information into an authentication credential container of a user. All that is taught is the use of certificates for authenticating a smart card, smart card application, terminal, and terminal application. Thus, contrary to the allegations in the Office Action, Li and Deo fail to teach or render obvious the specific features of claim 4.

With regard to claim 6, which is dependent from claim 3 discussed above, the alleged combination of references fails to teach or render obvious the features of the removing being performed automatically. The Office Action again points to the same sections of Li as cited for the features of claim 3, as allegedly teaching the features of claim 6. As mentioned above, these sections do not even teach the removal of access to

an application in a plurality of applications, let alone doing so automatically. Thus, contrary to the allegations in the Office Action, Li does not in fact teach or render obvious the specific features of claim 6.

Regarding claim 9, the alleged combination of references fails to teach or render obvious the feature of authentication information being injected into a separate hardware security device. The Office Action alleges that this feature is taught by Deo in the same sections as discussed above with regard to claim 4. It is clear that none of these sections mention anything regarding injecting authentication information, let alone injecting such authentication information into a separate hardware security device. All the cited sections of Deo teaches is the use of certificates for authenticating a smart card, smart card application, terminal, and terminal application. There is no injecting of authentication information into a separate hardware security device.

With regard to claim 21, the alleged combination of references fails to teach or render obvious the feature of the view comprising a list of keys employed by the user, wherein each entry in the list corresponds to a different key employed by the user, and wherein each entry identifies a type of the corresponding key and a serial number of the corresponding key. The Office Action alleges that these features are taught by Deo at the same sections as noted above with regard to claims 4 and 9. These sections only teach the use of certificates for authenticating a smart card, smart card application, terminal, and terminal application. There is no teaching of a view comprising a list of keys employed by a user. There is no teaching of the view having each entry corresponding to a different key employed by the user. There is no teaching that each entry identifies a type of the corresponding key. There is no teaching that each entry identifies a serial number of the corresponding key. These are very specific features and simply pointing to sections of Deo that teach authentication using certificates does not address these specific features of a view as recited in claim 21.

Regarding claim 22, the alleged combination of references fails to teach or render obvious the feature of the view comprising a profile of the user detailing a role of the user, a name of the user, contact information for the user, and employment information for the user. The Office Action alleges that these features are taught by Li at page 9, lines 4-14 which merely teaches that header information includes parameters such as User ID,

real name, user name, password, password timestamp, and agent privileges. There is no teaching here regarding a role of a user, contact information for the user, or employment information for the user. The only aspect of the view recited in claim 22 that is taught by the cited section of Li is a name of a user, but claim 22 does not only recite a name of a user. The view contains a profile having all of the elements recited in claim 22, not just one. Thus, the Office Action has not shown that Li teaches the features of claim 22.

With regard to claim 23, the alleged combination of references fails to teach or render obvious the feature of the view comprising a list of certificate-enabled applications accessible by the user, wherein each entry in the list corresponds to a different certificate-enabled application, and wherein each entry identifies a user name of the user and a last login attempt of the user for the corresponding certificate-enabled application. The Office Action alleges that the features of claim 23 are taught by Li at page 9, lines 4-14 and Deo at the same sections as addressed above. Li, page 9, lines 4-14 have been addressed above with regard to claim 22. This section of Li says nothing about the features of claim 23. Moreover, the cited sections of Deo, which are the same as addressed above with regard to claims 4 and 9, only teaches using certificates for authentication. There is nothing in either reference regarding the specific features of claim 23.

Regarding claim 25, the alleged combination of references fails to teach or render obvious the feature of the view comprising a list of personal applications accessible by the user, wherein each entry in the list corresponds to a different personal application, and wherein each entry identifies a number of accounts connected to the corresponding personal application. With regard to claim 27, the alleged combination of references fails to teach or render obvious the feature of the view comprising a user selectable graphical user interface element for invoking a function to delete a user name of the user from the list of certificate-enabled applications. The sections of the references cited as allegedly teaching the features of these claims are equally as irrelevant as the sections cited for each of the other dependent claims addressed above. The alleged combination of references simply fails to teach or render obvious the specific features recited in these claims.

The other claims recite additional features which, when taken alone or in combination with the features of the independent claims, are not taught or rendered obvious by the alleged combination of references. Thus, in addition to their dependency, the dependent claims are further distinguished over the alleged combination of references by virtue of the specific features recited in these claims.

III. Rejection under 35 U.S.C. § 103(a) Based on Li and Delany

The Office Action rejects claim 24 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Li et al. (Patent WO 98/26540) in view of Delany et al. (U.S. Patent Application Publication No. 2002/0138763). This rejection is respectfully traversed.

The distinctions over Li have been discussed above and are equally applicable to dependent claim 24. Moreover, Li does not teach or render obvious the specific features of claim 24, i.e. the features of the view comprising a list of enterprise applications accessible by the user, wherein each entry in the list corresponds to a different enterprise application, and wherein each entry identifies a user name of the user and a last login attempt of the user for the corresponding enterprise application. In addition, Delany, either alone or in combination with Li, does not teach or render obvious the features of claim 24.

The Office Action cites Li as teaching the majority of the features of claim 24 and cites Delany as allegedly teaching a last login attempt of a user. In actuality, Li does not teach any of the features of claim 24. The Office Action cites page 9, lines 4-14 of Li as allegedly teaching the features of claim 24 with the exception of the last login attempt. Page 9, lines 4-14 of Li teaches that the header information includes a name of a user, a user name or handle, a password, a password timestamp, and various agent privileges. Li makes no mention of enterprise applications accessible by a user or each entry in a list corresponding to a different enterprise application.

The Office Action cites paragraph [0428], lines 3-8 and paragraph [0429], lines 4-7 of Delany as teaching a last login attempt. Paragraph [0428], lines 3-8 of Delany discusses a login failure and logging login information. Paragraph [0429], lines 4-7 of Delany discusses logging an unsuccessful login. While Delany generally teaches logging

failed login attempts, neither Delany nor Li, either alone or in combination, teaches or renders obvious the specific features of a list of enterprise applications accessible by the user, wherein each entry in the list corresponds to a different enterprise application, and wherein ***each entry*** identifies a user name of the user and ***a last login attempt of the user for the corresponding enterprise application***.

Thus, in view of the above, Applicant respectfully submits that the alleged combination of Li and Delany fails to teach or render obvious the features of claim 24. Accordingly, Applicant respectfully requests withdrawal of the rejection of claim 24 under 35 U.S.C. § 103(a).

IV. Conclusion

It is respectfully urged that the subject application is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

Respectfully submitted,

DATE: October 6, 2010

Stephen J. Walder, Jr.
Reg. No. 41,534
WALDER INTELLECTUAL PROPERTY LAW, P.C.
17330 Preston Road, Suite 100B
Dallas, TX 75252
(972) 380-9475
ATTORNEY FOR APPLICANT